Penetration Testing

- 5 Days
- Lecture and Hands-on Labs

Course Overview

PEN-100 is designed to prepare students with the necessary prerequisites to enter into Penetration Testing with Kali Linux (PWK), also known as PEN-200. PEN-100 material is divided into Topics. Each Topic has multiple Learning Units, and a Learning Unit is a digestible, atomic piece of training that can be consumed within 1 to 3 hours on average, depending on the student. Each Learning Unit is defined by several Learning Objectives: discreet and practical goals for the student to strive for. Learning Objectives are assessed at the end of each Learning Unit via hands-on exercises. Many exercises require the student to show their skills by interacting with Offensive Security lab machines. The following syllabus contains the various Topics and Learning Units. Students are encouraged to consume the content in whichever order they wish, however, most students will benefit from following the prescribed order. A detailed syllabus of Learning Units and their Learning Objectives that will make up PEN-100 follows below.

Who Should Attend

- Penetration Testers
- Security Analysts
- Incident Responders
- Threat Intelligence
- Security Operations

What You'll Learn

- Linux Basics
- Windows Basics
- Networking Fundamentals
- Cryptography
- Web Applications
- Introduction to Active Directory
- Working with Shells
- Bash, Python, and PowerShell Scripting
- Troubleshooting

Outline

N-100 - 💻 Lecture + Lab: Meet VIRGIL: Your AI Lab Coach - General Introduction to PEN-100 - How to Learn - Introduction to Security Concepts - Practical Help Getting Started

2. Linux Basics - I

- Introduction to Linux
- Command Line Basics
- Manuals and Help

- The Linux File System
- Linux File Management
- Piping and Redirection
- Searching and Text Manipulation

3. Linux Basics - II

- Users and Groups
- File Permissions
- Linux Processes
- File and Command Monitoring
- Linux Applications
- Scheduled Tasks
- Logs
- Disk Management
- Linux Basics Cumulative Exercise

4. Windows Basics - I

- Linux vs. Windows
- Windows Shells
- Windows File System Navigation
- System Information and Environment Variables
- Managing Files from the Command Line
- Searching for Files and Text

5. Windows Basics - II

- Windows Access Controls and Security Principles
- Windows Local Accounts & Groups
- Windows Permissions
- Windows Processes
- Windows Libraries
- The Windows Registry
- Windows Scheduled Tasks
- Windows Disk Utilities
- Windows Basics I & II - Cumulative Exercise

6. Introduction to Networking

- The OSI Model
- The TCP/IP Model
- Network Protocols
- Data Packets and Analysis - I
- Data Packets and Analysis - II
- TCP/IP Helper Protocols
- Useful Network Technologies

7. Introduction to Scripting

- Scripting with Bash - I
- Scripting with Bash - II
- Scripting with Python - I
- Scripting with Python - II
- Scripting with Python - III

- PowerShell Basics - I
- PowerShell Basics - II

8. Linux Networking Tools - I

- Essential Networking Utilities
- Active Connections and Neighbors
- Routing and Network Troubleshooting
- Name Resolution
- Common Clients
- Netcat
- Socat
- HTTP
- DNS
- FTP

9. Linux Networking Tools - II

- ACLs Overview and Netfilter Introduction
- IPTables (Parameters, Modifying Rules with -A/-D/-I)
- IPTables (Extended Rules and Default Policies)
- UFW and FWBuilder
- Managing Network Services
- SSH
- HTTP
- FTP (pure-ftpd)
- Linux Networking Practical

10. Windows Networking Tools

- Essential Network Utilities
- Common Clients
- Firewalls
- Services
- Windows Networking - Cumulative Exercise

11. Introduction to Cryptography

- Cryptography Jargon
- Encoding Part I
- Encoding Part II
- Hashing
- Password Security
- Symmetric-Key Encryption
- Asymmetric-Key Encryption

12. Web Application Basics

- The OWASP Top Ten
- HyperText Transfer Protocol
- HTTP Proxying and Burp Suite
- HTTP Methods and Responses
- HTTP Headers
- Browser Development Tools, HTML, and CSS
- Introduction to Javascript

- HTTP Routing
- Introduction to Databases and SQL

13. Network Scripting

- Writing a Client Program with Python - I
- Writing a Client Program with Python - II
- Writing a Server Program with Python
- Writing a Port Scanner with Python
- Website Interaction with Python - I
- Website Interaction with Python - II
- Capturing and Sending Packets with Scapy

14. Introduction to Active Directory

- Active Directory Introduction
- Active Directory Elements
- Administrating AD

15. How to Learn Troubleshooting

- Introduction to Troubleshooting
- Misaligned Instructions
- A Basic Python Coding Error
- Finding a Broken Exploit
- Network Troubleshooting
- Accidental File Deletion

16. Introduction to Nmap

- Understand what Nmap is
- Perform basic Nmap usage
- Use options in Nmap
- Utilize Nmap input and output files
- Create Nmap Script Engine (NSE) scripts
- Assess Nmap traffic

Prerequisites

- None